secorvo
security consulting

Secorvo Security News

Februar 2007

Editorial: Gedankenverbrechen

Vor allem drei Zukunftsvisionen haben in den vergangenen 100 Jahren die Gemüter bewegt: die „Schöne neue Welt“ von Aldous Huxley (1932), der Roman „1984“ von George Orwell (1948) und „Fahrenheit 451“ von Ray Bradbury (1953). Allen gemeinsam ist die düstere Prognose, dass eine autoritäre, anonyme und technokratische Herrschaftsform unter Nutzung modernster Technik die Menschen zu dumpfen, würdelosen Marionetten degradieren wird.

Der wesentliche Unterschied: Sah Huxley die Bedrohung in einer fortschreitenden Abstumpfung durch Amüsement, Drogenkonsum (Soma) und gezielte Embryonenmanipulation, zeichnet Orwell einen totalen Überwachungsstaat, der mittels Gedankenpolizei und Televisoren, die öffentliche Plätze und Wohnungen ausleuchten, keinen Raum für Privatsphäre lässt. In Bradburys Vision kommt beides zusammen: Bücher sind verboten und werden öffentlich verbrannt, das Volk schluckt Glückspillen und amüsiert sich vor Videowänden.

Es schien, als habe Huxley die Zukunft treffender prognostiziert: „Big Brother“ ist heute die Marke einer Fernsehshow, über die die Welt lacht. In „Wir amüsieren uns zu Tode“ beschrieb der Medienwissenschaftler Neil Postman 1985 Desinformation und Abstumpfung durch Fernsehkonsum. Dabei waren es 1988 „nur“ 2,5 Stunden; 2002 verbrachten die Deutschen durchschnittlich 3,5 Stunden pro Tag vor dem Fernseher – das sind 160 Acht-Stunden-Tage pro Jahr. Zugleich steigt die Analphabetenquote: 2004 galten 6,5-11% der Deutschen als „funktionale Analphabeten“ – das sind 4-7 Mio. Menschen.

Nun aber holt Orwell auf. Nach „großem Lauschangriff“, Vorratsdatenspeicherung und der Zunahme der Abhöranordnungen steht nun die „Online-Durchsuchung“ auf der Agenda. Neusprech vom Feinsten: Im Unterschied zur echten Durchsuchung erfolgt sie heimlich.

In „1984“ blieb Winston Smith eine Ausflucht: ein Tagebuch, in dem er in einer nicht einsehbaren Ecke seines Zimmers seine „Gedankenverbrechen“ notierte. 2007 dürfte er dafür keinen PC verwenden.

Inhalt

secorvo
security consulting

Security News

Anti-Spyware – Best Practices

Die Anti-Spyware Coalition (ASC) ist eine Initiative von derzeit knapp 50 Mitgliedsunternehmen, die sich 2005 zur Bekämpfung von Spyware und anderer unerwünschter Software zusammengeschlossen haben.

Am 25.01.2007 veröffentlichte die ASC den Guide Best Practices: Factors for Use in the Evaluation of Potentially Unwanted Technologies. Darin werden Anti-Spyware-Herstellern Hinweise gegeben, nach welchen Kriterien Software als „unerwünscht" bewertet werden kann. Diese Hinweise sollten von allen Softwareherstellern als Orientierung genutzt werden, um Fehleinordnungen zu verhindern. Denn einer zentralen Grundforderung der ASC ist nichts hinzuzufügen: „Users should be in control of their computers at all times." (Benutzer sollen zu jeder Zeit wissen, was auf ihren Rechnern passiert.)

Fast ausnahmslos betroffen

Die am 31.01.2007 von der Information Systems Security Association (ISSA) und dem University College Dublin (UCD) veröffentlichte Studie „Irish Cybercrime Survey 2006" bringt ein erschreckendes Ergebnis zu Tage: 98% der befragten Firmen gaben an, von Sicherheitsvorfällen betroffen gewesen zu sein.

Auch wenn mit 42 Organisationen – von kleinen irischen Firmen über öffentliche Einrichtungen bis zu großen Konzernen – nur eine vergleichsweise kleine Stichprobe erhoben wurde, sind die Ergebnisse der Studie und die Aufschlüsselung der einzelnen Vorfälle sehr informativ.

Globaler Überblick

Seit dem 05.02.2007 ist das Active Threat Level Analysis System (ATLAS) von Arbor Networks auch für die breite Öffentlichkeit verfügbar und stellt damit als Expertensystem im Gegensatz zu anderen kommerziellen Diensten erstmals auch Privatpersonen statistisches und technisch detailliertes Datenmaterial zu aktuellen Angriffen kostenlos zur Verfügung.

Technisch basiert es auf einem Sensornetzwerk, das ca. 70% des Internet abdeckt. Die diesen Auswertungen zu Grunde liegenden Daten stammen u. a. aus Honeynetködern, eingefangener und analysierter Malware, Logs von Intrusion Detection Systemen und Netzwerkscans, Statistiken zu Denial-of-Service, ermittelten Daten zu Phishinginfrastrukturen und Botnet Command & Control sowie Nachrichten- und Schwachstellenmeldungen.

Damit wird ein komprimierter Echtzeitüberblick über die globalen Sicherheitsereignisse und -trends gegeben. So ist es möglich, auf einen Blick 24-Stunden-Zusammenfassungen sortiert nach aktuellen Angriffstypen oder regionalen Aktivitäten zu erhalten. Festgestellte automatisierte Scans werden u. a. nach Service/Port, Ausgangsland und Autonomous System Number aufgeschlüsselt.

Sehr aussagefähig ist auch der Risikoindex, der existierende technische Schwachstellen in Relation zu ihrer Ausnutzbarkeit und Verbreitung im Internet sowie den tatsächlich beobachteten Angriffen nach dem Common Vulnerability Scoring System bewertet. Dieses neue Informationsangebot ist hervorragend geeignet, kommerzielle Sicherheitsmeldungen zu verifizieren und die externen Bedrohungen, denen der eigene Arbeitsbereich ausgesetzt ist, objektiver zu bewerten.

FIPS-Validierung für OpenSSL

Am 06.02.2007 gab das Open Source Software Institute (OSSI) die erneute FIPS 140-2 Validierung des OpenSSL FIPS Object Modules bekannt. Die Validierung ist in den USA erforderlich, um Open Source Software für die Verarbeitung sensibler Daten bei US Behörden einsetzen zu dürfen.

Der Validierungsprozess dauerte statt der üblichen wenigen Monate mehr als fünf Jahre. Das lag zum Einen daran, dass kein Binärcode, sondern Source Code vom Computer Module Validation Program (CMVP), einem Joint Venture des US-amerikanischen National Institute of Standards and Technology (NIST) und des kanadischen Communications Security Establishment (CSE), geprüft werden musste – eine solche Prüfung hat es noch nie gegeben. Zum anderen wurde der Validierungsprozess von anderen kommerziellen Herstellern, die ähnliche Produkte vertreiben, durch zahlreiche Eingaben boykottiert. So musste die Validierung im Juli 2006 zunächst zurückgezogen werden, da Hersteller massive anonyme Beschwerden bei der CMVP eingereicht hatten.

Zwar wurde die Validierung letztlich erfolgreich abgeschlossen, aber die überprüfte Version ist mehr als drei Jahre alt. Dennoch enthält sie u. a. bereits die Hashfunktionen SHA-224, SHA-256, SHA-384 und SHA-512.

„Ist Fatalismus angebracht?"

Dies war eine der zahlreichen Fragen, die auf dem mittlerweile 14. DFN-CERT Workshop „Sicherheit in vernetzten Systemen" diskutiert wurden, der am 07. und 08.02.2007 stattfand – wie immer in Hamburg. Johannes Strümpfel stellte diese Frage in seinem sehr spannenden Abschlussvortrag „Werk-

zeuge der Industriespionage“ – und verneinte sie trotz etlicher beeindruckender Beispiele aus der Welt des „Cyber Crimes“.

Auch die anderen Vorträge der zweitägigen Veranstaltung präsentierten den auch in diesem Jahr über 300 Teilnehmern unterschiedliche Themen der System- und Netzwerksicherheit – von technischeren Aspekten (Joanna Rutkowska: „Fighting Stealth Malware – Towards Verifiable OSes“) über Fragen der sicheren Softwareentwicklung (Martin Johns: „CISAT: Integration von sicherheitszentrierter statischer Analyse in den Entwicklungsprozess“) bis zu sehr anschaulich vorgetragenen, aktuellen rechtlichen Fragestellungen (Heidi Schuster: „Wikis und Foren – Möglichkeiten eines rechtskonformen Betriebs“).

Fast alle Folien stehen zum Download bereit; in Kürze werden ferner die während des Workshops live im Internet übertragenen Vorträge als Aufzeichnungen verfügbar sein.

Viel hilft viel – aber wem?

Auf der am 09.02.2007 zu Ende gegangenen RSA Conference 2007 wurde ein Großangebot aus zahllosen Keynotes, 19 fachlichen Schwerpunktthemen und über 220 Einzelvorträgen zu allen erdenklichen Aspekten der IT-Sicherheit geboten. Die Kernbotschaft an die Teilnehmer nahm sich jedoch eher schlicht aus: die alten Probleme sind auch die neuen – Malware, Rootkits, Botnets vereint unter einer steuernden und kreativen Online-Kriminalität.

Ob PC, Handy, Spieleconsole oder zukünftig der Kühlschrank: Angreifer werden in allen Systemen Schwachstellen finden. Diese Entwicklung ist nach Aussagen führender Sicherheitsexperten wie Vint Cerf und Eugene Kaspersky unumkehrbar.

Dementsprechend war das Ausstellungsangebot eher auf technische als auf strategisch-organisatorische Schutzlösungen ausgerichtet.

Folgt aus solchen Aussagen der IT-Sicherheitsindustrie, dass IT-Sicherheit zukünftig nur noch von (großen) Herstellern "miteingekauft" werden kann? Da sollte man es wohl besser mit den Römern halten und sich fragen: Quis custodit custodes? (Wer überwacht die Wächter?). Die resignativen Tendenzen stimmen bedenklich – und sichere Softwareentwicklung ist bislang keine Stärke der Software-Anbieter.

Machen 123 Mio. € sicherer?

Am 24.01.2007 wurde durch den Beschluss des Bundeskabinetts im Forschungsbereich „Neue Technologien“ des BMBF das Rahmenprogramm „Sicherheitsforschung – Forschung für die zivile Sicherheit“ aufgelegt. Bis zum Jahr 2010 ist es mit rund 123 Mio. Euro budgetiert und verfolgt mit seinen zwei Programmlinien „Szenarienorientierte Sicherheitsforschung" und „Erforschung von Querschnittstechnologien in Technologieverbünden“ das Ziel, die zivile Sicherheit präventiv zu erhöhen, ohne dadurch die Freiheit der Bürgerinnen und Bürger einzuschränken. Erreicht werden soll dies durch innovative organisatorische Konzepte und Handlungsstrategien. Insbesondere den Quellen von Bedrohungen, dem Datenschutz und den Auswirkungen auf die Menschen- und Freiheitsrechte wird in der Zielsetzung ein hoher Rang eingeräumt.

Ob diese heren Ziele erreicht werden, bleibt abzuwarten. Denn wo viel Geld ist, ist auch viel Schatten: Die Verantwortlichen werden dazu in der Auseinandersetzung mit den um diese Forschungsgelder buhlenden Interessensgruppen sehr standhaft bleiben müssen.

DuD 2007

Knapp drei Wochen noch bis zur diesjährigen Fachtagung „DuD 2007“ am 12.-13.03.2007 in Berlin – zwei Tage mit spannenden, prominent besetzten Vorträgen rund um IT-Sicherheit und Datenschutz unter der Leitung der Herausgeber der Fachzeitschrift DuD, Dr. Johann Bizer und Dirk Fox. Thematische Schwerpunkte bilden in diesem Jahr die Sicherheit von Web-Applikationen und die ID-Strategie der Bundesregierung. Programm und Online-Anmeldung unter www.computas.de.

Secorvo News

Secorvo College aktuell

Der T.I.S.P.-Schulungstermin am **05.–09.03.2007** ist fast ausgebucht – es gibt nur noch zwei freie Plätze für Kurzentschlossene.

Aufgrund der großen Nachfrage nach dem T.I.S.P.-Zertifikat wird Secorvo eine zusätzliche T.I.S.P.-Schulung in der ersten Jahreshälfte anbieten. Der Termin wird in Kürze auf der Webseite von Secorvo College veröffentlicht. Wenden Sie sich bei Interesse bitte bis dahin an college@secorvo.de.

Programm, Preise und Online-Anmeldung für die Seminare

- PKI – Grundlagen, Vertiefung, Realisierung
  am **26.–29.03.2007**,
- IT-Sicherheitsaudits in der Praxis
  am **17.–19.04.2007** und
- Sichere Softwareentwicklung
  am **24.–26.04.2007**

finden Sie unter www.secorvo.de/college.

Veranstaltungshinweise

Auszug aus www.veranstaltungen-it-sicherheit.de

Februar 2007	
26.-27.02.	Net-ID 2007 (Computas, Berlin)
März 2007	
05.-09.03.	TISP-Schulung (Secorvo College, Karlsruhe)
10.03.	TISP-Prüfung (Secorvo College, Karlsruhe)
12.-13.03.	DuD 2007 (Computas, Berlin)
26.-28.03.	Fast Software Encryption 2007 (IACR, Luxembourg)
26.-29.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)
27.-30.03.	Black Hat Europe 2007 (Black Hat, Amsterdam)
April 2007	
17.-19.04.	IT-Sicherheitsaudits in der Praxis (Secorvo, Karlsruhe)
24.-26.04.	Sichere Softwareentwicklung (Secorvo, Karlsruhe)
Mai 2007	
22.-24.05.	10. Deutscher IT-Sicherheitskongress (BSI, Bonn)

Fundsache

Auszug aus www.security-finder.de

Im Dokument „The Nepenthes Platform: An Efficient Approach to Collect Malware“ präsentieren die Autoren einen neuartigen Ansatz zur automatisierten Sammlung von Viren, Würmern und Trojanern: auf einem Server werden Netzwerk-Protokolle emuliert, die typischerweise von Schad-Software zur Verbreitung verwendet werden. Auf diese Weise kann Malware "gefangen" und anschließend analysiert werden.

Impressum

http://www.secorvo-security-news.de/

ISSN 1613-4311

Redaktion: Petra Barzin, Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de